Juan Antonio Suárez Suárez

Ingeniería de la Ciberseguridad

Móstoles, Madrid (ES) · +34 676273835 · juan_srz95@hotmail.com
Website(s): LinkedIn · www.linkedin.com/in/jasrz
HTB · https://app.hackthebox.com/profile/1110809
Github · https://github.com/juansrz
Portfolio · https://juansrz.github.io/

Resumen

Estudiante de Ingeniería de la Ciberseguridad (URJC) con experiencia práctica en detección y respuesta (Wazuh + ELK, análisis de logs y hardening Linux) y en reversing/exploit (radare2, ROP/shellcode, fuzzing con AFL++). He trabajado corrigiendo vulnerabilidades en Java/Spring Security apoyándome en SonarQube, automatizando tareas con Python/Bash/Docker y resolviendo laboratorios y CTFs en plataformas como Hack The Box. Busco mis primeras prácticas en ciberseguridad, abierto a distintas áreas técnicas (SOC, pentesting, AppSec...) donde seguir aprendiendo y aportar rigor técnico, buena documentación y capacidad de análisis.

Habilidades y Herramientas

- Blue Team / Detección: SIEM (Wazuh, Elastic/ELK), ingestión y parsing de logs, creación de reglas y paneles, hardening Linux básico, documentación de incidentes.
- Pentesting / Red Team (junior): Nmap, Wireshark, enumeración de servicios, scripting en Bash/Python para reconocimiento; Burp Suite
- Reversing & Exploit Dev: radare2, ROPgadget, ingeniería inversa básica, AFL++ (fuzzing), desarrollo de shellcode AMD64, cadenas ROP y uso de mprotect().
- Dev & Data: Python, Bash, C, Java, Flask, SQLite, scikit-learn (clasificación), Jinja2/xhtml2pdf (informes), Git, Docker.
- Redes / Sistemas: TCP/IP, DNS, DHCP, VLAN; Linux (Kali/Ubuntu) y Windows; regex; YARA.

Proyectos

ipLog.sh (Bash) — Analizador de *auth logs* con soporte `*.log` y `*.log.gz`, **validación robusta de IPs**, búsqueda optimizada, manejo de permisos/errores y salida legible. ➜ Detección de IPs sospechosas y reporte.
https://github.com/juansrz/ipLog

Lab SIEM: Wazuh + Elastic — Ingesta de logs de sistema, reglas básicas de alerta, dashboards y simulación de eventos. Documentación de casos de uso **SOC L1**.
https://github.com/juansrz/siem-lab-wazuh-elk

Hardening WebGoat con SonarQube (Spring Security) — Mitigación de findings (p. ej., uso inseguro de `PasswordEncoder`), refactor y verificación en SonarQube; notas y evidencias.
https://github.com/juansrz/WebGoat

Minishell (C) — Shell tipo Unix con pipes/redirecciones y **corpus de entradas (fuzzing corpus)** para estrés de parsing (casos borde).
https://github.com/juansrz/minishell-ssoo-urjc

ROP + shellcode AMD64 (Docker) — Cadena **ROP** para invocar `mprotect()` y ejecutar **shellcode** desde nuevo stack; extracción de gadgets con **ROPgadget** y verificación con **radare2**.
https://github.com/juansrz/malware-p3-rop-mprotect

CTF MDS – Automatización web y PRNG — Bots Selenium para retos tipo “10 Fast Fingers” y “Whack-a-Mole”, explotación de PRNG con semilla `System.currentTimeMillis()` (CWE-337) en el reto “La Lotería” y refactor/test de `SecureCalculator` con JUnit 5 + Mockito.
https://github.com/juansrz/mds-practica2-ctf

Formación

URJC — Grado en Ingeniería de la Ciberseguridad · *2018 – 2026*

Asignaturas y prácticas destacadas: Metodologías de Desarrollo Seguro, Malware y Amenazas Dirigidas, IA (búsqueda, redes bayesianas, Naive Bayes), Sistemas Operativos (Bash, procesos/threads, planificación), Arquitectura (cachés), Estructuras de Datos.

C.E.S Juan Pablo II — C.F.G.S Mantenimiento de aviónica · *2015 – 2017*

Experiencia

Mercadona — Gerente A · Madrid · *2019 – 2024*

- Gestión diaria de inventario y reposición; mejora de la trazabilidad y reducción de incidencias mediante checklists y métricas simples.
- Coordinación de equipo y cumplimiento de estándares de calidad/seguridad operativa; resolución de incidencias y reporte claro.
- Optimización de tiempos de reposición y disminución de roturas aplicando procedimientos y verificación cruzada.

Iberia Maintenance — Técnico de mantenimiento de aeronaves · Madrid · *2017 – 2018*

- Inspección/desmontaje (p. ej., RB211), control de calidad en taller y hangar; cumplimiento estricto de checklists y normativa.
- Operaciones de inspección y control, operaciones de recambio y desmontaje, operaciones de mantenimiento, reparación e intercambio de componentes (neumáticos, llantas, aviónica y salvamento), siguiendo procedimientos estrictos de seguridad y calidad.

Idiomas/Otros

Español: nativo

Inglés: B2

Otros: Permiso de conducir B/A1 y vehículo propio

Disponibilidad para incorporación inmediata